[0015] FIGS. **4**, **5**, **6**, and **7** each illustrate aspects of internal security issues addressed using the exemplary embodiments of the invention; and

[0016] FIG. **8** is a logic flow diagram that illustrates the operation of a method and a result of execution of computer program instructions embodied on a computer readable medium, in accordance with exemplary embodiments of this invention.

DETAILED DESCRIPTION

[0017] The exemplary embodiments of the invention provide at least a method to provide cloud centric trust validation including deploying sensitive applications to a public cloud by utilizing a model and pushing master keys to the cloud from a trusted zone such as within a corporate network.

[0018] Current state of technology depends on encryption operations and key management systems deployed within public cloud environments and/or leveraging trust validation solution that exclusively or significantly depend on validation of applications from within the public cloud. Both of these factors will pose various security and compliance risks to users and other entities.

[0019] Establishing trust between cloud applications and corporate network is usually done using 'pull' mechanism, where cloud application connects to a corporate network and identifies itself with specific authentication information such as SSH keys or other credentials. The challenge in this kind of model is how to deliver that authentication information to cloud applications in the first place. Previous solutions have not been very secure (because of a chicken-and-egg type of situation) or they've been very dependent on specific cloud provider security controls. The exemplary embodiments of the invention provide at least a method and apparatus to 'push' master keys generated for a private network, such as a corporate network, for establishing a most secure trust between the cloud applications and the corporate network.

[0020] FIG. **1** illustrates a general overview of components and entities which the exemplary embodiments of the invention can benefit. As illustrated in FIG. **1** there is a public cloud **100**. There is illustrated within the public cloud **100** a cloud infrastructure provider **110** and a cloud instance **120**. The cloud instance **120** can be representative of an application instance as will be discussed in more detail herein. In addition, in FIG. **1** there is a private cloud **150**. There is illustrated within the private cloud **150** an application provisioning agent corporate enterprise **170**, an application repository **160**, and an application secrets repository **180**. The exemplary embodiments of the invention enable secure application instance deployment in a public cloud by an application provisioning agent of a private network such as in the private cloud **150**. The exemplary embodiments of the invention enable a private entity to utilize the public cloud to deploy applications in a public cloud safely using approach where the use of the application instances and the security elements of the connection are made much more secure for a device using the application in the public cloud. The exemplary embodiments further enable at least an establishment of a master key which is created and/or selected by the private network for the use and authentication of the application.

[0021] This invention presents a model where only non-sensitive information is required to be stored to cloud and using that, public and non-sensitive information, corporate network can safely and securely deploy new applications by pushing the required master keys to new cloud instances. Exemplary embodiments of the invention are described in at least FIGS. **3**A and **3**B.

[0022] Although the invention may be described and/or illustrated using references to particular entities such as Nokia® and Amazon® the use of these entities is non-limiting and the invention can be practiced to the benefit of any entities which incorporate similar technology.

[0023] In accordance with an exemplary embodiment of the invention which will be described in more detail below there is at least a method to deploy sensitive applications to a public cloud by utilizing a model where master keys are pushed to the cloud from a trusted zone such as within a corporate network.

[0024] Before describing in further detail the exemplary embodiments of this invention reference is made to FIG. **2** for illustrating a simplified block diagram of various electronic devices and apparatus that are suitable for use in practicing the exemplary embodiments of this invention.

[0025] The server **22** of FIG. **2** can be associated with a public cloud **200**. The server **22** includes a controller, such as at least one computer or a data processor (DP) **22**A, at least one computer-readable memory medium embodied as a memory (MEM) **22**B that stores a program of computer instructions (PROG) **22**C, and at least one suitable RF transceiver **22**D for communication with the ED **21** via antennas **21**F (several when MIMO operation is in use). The server **22** is coupled via a data/control path **212**F to the ED **21**. The path **212**F may be implemented such as by a wired and/or wireless connection. The server **22** can also be coupled to another device, such as via the data/control path **215**F to the KMS **23**.

[0026] The ED **21** includes a controller, such as at least one computer or a data processor (DP) **21**A, at least one non-transitory computer-readable memory medium embodied as a memory (MEM) **21**B that stores a program of computer instructions (PROG) **21**C, and at least one suitable radio frequency (RF) transmitter and receiver pair (transceiver) **21**D for bidirectional wireless communications with the key management system **23**, the application server **22**, and/or another device associated with the cloud via an antenna or antennas **21**F, and/or a hardwired connection. In addition the KMS **23** may be directly or indirectly connected to the ED **21** such as via a connection **222**F.

[0027] For the purposes of describing the exemplary embodiments of this invention the application server **22**, the application provider device **21**, and/or the key management system **23** may be assumed to include a trust establishmnent function (TEF). The TEF **21**G, TEF **22**G, and/or the TEF **23**G are assumed to be configured to operate in accordance with the non-limiting examples of the embodiments of this invention as described herein.

[0028] At least one of the programs **21**C, **22**C, and **23**C is assumed to include program instructions that, when executed by the associated data processor, enable the device to operate in accordance with the exemplary embodiments of this invention, as will be discussed below in greater detail. That is, the exemplary embodiments of this invention may be implemented at least in part by computer software executable by the DP **21**A, DP **22**A, and/or DP **23**A, or by hardware, or by a combination of software and hardware (and/or firmware). Likewise, the TEF **21**G, TEF **220**, and the TEF **23**G may be implemented at least in part by executable computer software, or by hardware, or by a combination of software and hardware (and firmware).